Intrusion Detection and Information Security Audits

Terry T. Kidd
University of Texas Health Science Center, USA

Robert K. Hiltbrand
University of Houston, USA

INTRODUCTION

The rapid expansion and dramatic advances in information technology in recent years have without question generated tremendous benefits to business and organizations. At the same time, this expansion has created significant, unprecedented risks to organization operations. Computer security has, in turn, become much more important as organizations utilize information systems and security measures to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information. Such use of computer security is essential in minimizing the risk of malicious attacks from individuals and groups. To be effective in ensuring accountability, management and information technology security personnel must be able to evaluate information systems security and offer recommendations for reducing security risks to an acceptable level. To do so, they must possess the appropriate resources, skills, and knowledge.

With the growing perverseness of information systems and the technologies used to support such tools, the growing need to keep the integrity of both the data and the system used to manage that data will become a major priority. Therefore, it is important for security personnel and management to keep abreast of the issues and trends in information systems and security, and the tools and techniques used to secure systems and data.

In order to keep information safe and systems secured from outside attacks from computer criminals, information systems security and network vulnerability assessment must be conducted on a regular and ongoing basis to insure system security integrity. The aim of this article is to introduce to the information technology community, the conceptual overview of information security audits. Not only will this article present an overview of information security audits, but also information on popular intrusion detection and security auditing software used in industry.

BACKGROUND

Advances in information systems and the technology used to support those systems have produced great results for organizations, businesses, and other agencies in terms of work productivity, information storage, management, and in opportunities for the competitive advantage. While the promise and offerings of information systems have tremendous benefits, information systems have also created significant and unprecedented levels of risks to organizational operations. Businesses, hospitals, schools, universities, governmental agencies, and banks depend heavily on information systems, thus increasing the need for information security. With this newfound dilemma, organizations are beginning to use information security measures to ensure that the integrity of other data is held at an optimal level.

As discussed previously, the aim of information security used by an organization is to avoid data tampering, fraud, inappropriate access to and disclosure of sensitive information, and disruptions in critical operations (Umar, 2003). Unfortunately, these risks are expected to escalate as wireless communication technologies emerge and become ubiquitous. If information systems personnel are to be effective instruments of accountability and assessment, they need to be able to evaluate information systems and security measures to offer recommendations for reducing the security risk to an acceptably low level (Umar, 2003).

Further, the growing importance of information systems in performing daily operational activities, along with the elimination of paper-based evidence and audit trails, demands that these professionals consider the effectiveness of information technology security

controls during the course of financial and performance audits. To do so, information security personnel must acquire and maintain appropriate resources and skill sets to help prevent computing security threats, vulnerabilities, or attacks. This can be a daunting challenge in an era of rapid evolution and deployment of new information technology. Likewise, management within organizations needs to take stock of their information systems security audit and its capabilities, to ensure that strategies exist for their continued development and enhancement, for an organization's security is only as strong as its policy.

When it comes to articulating or writing the organization security policy, the discussion should be more than information systems and the technologies used to support those systems, the conversation should move past a discussion of infrastructure (e.g., hardware and software), but to a discussion of security and methods for securing the organization's systems and most valuable assets—its information.

According to Holden (2004), information is essential to the achievement of any business or organizational. Its reliability, integrity, and availability are significant concerns in most organizations. The use of computing and system networks, particularly the Internet, is revolutionizing the way organizations conduct their business and their day-to-day operations. While the benefits of such tools have been enormous and have allowed vast amounts of information to be available at our fingertips, these interconnections also pose significant risks to computer systems, information, and to the critical operations and infrastructures they support. Infrastructure elements such as telecommunications, power distribution, financial data, research and development information, as well as personnel data are subject to these risks. The same factors that benefit operations—speed and accessibility—if not properly controlled, can leave them vulnerable to fraud, sabotage, and malicious or mischievous acts (NSAA & GAO, 2001). In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected. Recent publicized disruptions caused by virus, worm, and denial of service attacks on both commercial and education Web sites illustrate the potential for damage.

Information security is of increasing importance to all levels of organization management in minimizing the risk of malicious attacks from individuals and groups. These risks include the fraudulent loss or misuse of organization resources, unauthorized access to release of sensitive information such as tax and medical records, disruption of critical operations through viruses or hacker attacks, and modification or destruction of data. According to the National State Auditing Association and the General Accounting Office (NSS & GAO, 2001), the risk that information attacks will threaten vital organization interests increases with the following developments in information technology:

- Monies are increasingly transferred electronically between and among governmental agencies, commercial enterprises, businesses, and individuals.
- Organizations and businesses are rapidly expanding their use of electronic commerce.
- Business, government, and national/domestic security communities increasingly rely on the available information technology.
- Public utilities and telecommunications increasingly rely on computer systems to manage everyday operations.
- More and more sensitive economic and commercial information is exchanged electronically.
- Computer systems are rapidly increasing in complexity and interconnectivity.
- Easy-to-use hacker tools are readily available, and hacker activity is increasing.
- Paper supporting documents are being reduced or eliminated.
- Each of these factors significantly increases the need for ensuring the privacy, security, and availability of state and local government, business, and public education systems.

Although as many as 80% of security breaches are probably never reported, the number of reported incidents are growing dramatically with relative intensity (NSAA & GAO, 2001). To further illustrate the need for information systems security, a survey conducted by the Computer Security Institute in cooperation with the FBI found that 70% of respondents from large corporations and government agencies had detected serious computer security breaches within the last 12 months and that quantifiable financial losses had increased over past years (NSAA & GAO, 2001).

Are organizations responding to the call for greater security? There is great cause for concern regarding this